1. Residui ed equazioni diofantee

1.1 Equazioni diofantee non lineari

In quasi tutte le competizioni matematiche, la componente della teoria dei numeri richiede spesso al risolutore l'approccio a equazioni diofantee[1], ossia equazioni in cui tanto le incognite quanto i coefficienti sono interi (o al più razionali), e possono presentare gradi di difficoltà, a seconda di come sono strutturate, ampiamente differenti. E molte volte tale difficoltà risiede nel dimostrare l'impossibilità dell'equazione stessa, ossia l'assenza di soluzioni.

È bene sottolineare prima di tutto che risolvere un'equazione diofantea in n incognite consiste nel trovare *tutte e sole* le n-uple di numeri interi che la verificano. L'espressione "tutte e sole" ha il significato che di seguito illustriamo. Sia Δ l'equazione diofantea data e sia S l'effettivo insieme delle soluzioni di Δ. Allora

(a) "trovare *tutte* le soluzioni" significa dimostrare che se $\overline{\mathrm{x}} = (\overline{x}_1, \ldots, \overline{x}_n)$ è una soluzione di Δ, allora $\overline{\mathrm{x}} \in S$;

(b) "trovare le *sole* soluzioni" significa dimostrare che se $\overline{\mathrm{x}} = (\overline{x}_1, \ldots, \bar{x}_n) \in S$, allora $\overline{\mathrm{x}}$ è una soluzione di Δ.

[1] Il termine "equazione diofantea" o "equazione diofantina" trae origine dal matematico Diofanto di Alessandria, vissuto in Egitto tra il III e il IV secolo d.C.

Prendiamo l'esempio dell'equazione diofantea

$$\Delta : x^2 - y^2 = 1.$$

Dimostriamo che l'insieme delle soluzioni coincide con $S = \{(1,0),(-1,0)\}$. Infatti

(a) se $(\overline{x},\overline{y})$ è una soluzione di Δ allora deve accadere che $\overline{x}^2 - \overline{y}^2 = 1$, ossia $(\overline{x}-\overline{y})(\overline{x}+\overline{y}) = 1$ che ha come due uniche possibilità

$$\begin{cases} \overline{x}-\overline{y} = 1 \\ \overline{x}+\overline{y} = 1 \end{cases} \quad \text{e} \quad \begin{cases} \overline{x}-\overline{y} = -1 \\ \overline{x}+\overline{y} = -1. \end{cases}$$

I due sistemi forniscono, rispettivamente, le soluzioni $(1,0)$ e $(-1,0)$. Abbiamo quindi ottenuto che necessariamente $(\overline{x},\overline{y}) \in S$;

(b) viceversa, se la coppia $(\overline{x},\overline{y}) \in S = \{(1,0),(-1,0)\}$, allora risolve l'equazione. Infatti $1^2 - 0^2 = 1$ e $(-1)^2 - 0^2 = 1$.

In realtà nella maggior parte dei casi il grosso del lavoro viene svolto dal primo punto, che consiste nel cercare di capire come sono fatte le soluzioni richieste. Il secondo punto, di conseguenza, si riduce a verificare che le soluzioni "provvisorie" verifichino effettivamente l'equazione data.
Veniamo ora, nello specifico, a trattare le equazioni diofantee non lineari, ovvero quelle equazioni a coefficienti e incognite interi che non sono in forma polinomiale, oppure che, se sono in forma polinomiale, non hanno grado pari a 1.
L'utilizzo delle congruenze nella risoluzione delle equazioni diofantee ha principalmente le seguenti finalità:

- dimostrare l'impossibilità di un'equazione;
- ricavare informazioni di divisibilità sulle variabili in gioco;
- scrivere le soluzioni in forma parametrizzata (dipendenti da un parametro).

Vediamo, ad esempio, come sia possibile dimostrare l'impossibilità di un'equazione, considerando la diofantea

$$x^2 + 3y = 2.$$

Analizzandola modulo 3, si evince immediatamente che dev'essere $x^2 \equiv 2 \pmod 3$. Ma ciò è assurdo, in quanto i residui quadratici modulo 3 sono solo 0 e 1. E siccome l'uguaglianza implica la congruenza, si ha che l'impossibilità in termini di congruenze implica l'impossibilità in termini di uguaglianze[2], ossia l'equazione è impossibile.

[2]Si sta dicendo, col linguaggio della logica matematica, che, fissati a, b, m interi, la proposizione $a = b \Rightarrow a \equiv_m b$ è equivalente alla sua contronominale, ossia $a \not\equiv_m b \Rightarrow a \neq b$

Vediamo invece come l'utilizzo dell'aritmetica modulare permetta di ottenere delle informazioni di divisibilità sulle incognite. Prendiamo, per esempio, l'equazione

$$6^x - 7y = 22.$$

Ragionando modulo 7 si ottiene che $6^x \equiv 1 \pmod 7$, ossia $(-1)^x \equiv 1 \pmod 7$, da cui è facile ricavare $x \equiv 0 \pmod 2$, cioè che x sia pari. Si è dunque ricavata un'informazione intermedia, che potrà essere utile successivamente per restringere il campo di ricerca delle soluzioni.
A volte accade, invece, che l'utilizzo di alcuni moduli non porti a nessuna nuova informazione. Ad esempio, partendo dall'equazione $4^x - 3y^2 = 7$ (da risolvere negli interi positivi), ragionando modulo 3 si ottiene che $1^x - 0 \equiv 1 \pmod 7$, che è verificata qualunque sia la scelta di x intero e dunque non concorre a fornire un'ulteriore informazione sull'incognita.
In svariate circostanze occorre dunque, una volta appurato che l'utilizzo di un certo modulo non dà informazioni utili sulle incognite, tentare con moduli diversi. Ad esempio, sempre a partire dall'equazione $4^x - 3y^2 = 7$, una volta appurato che la scelta del modulo 3 si rivela inefficace, potrebbe sembrare opportuno agire modulo 4. E infatti si ha che $0 - 3y^2 \equiv 3 \pmod 4$, ossia $y^2 \equiv -1 \pmod 4$, fatto assurdo in quanto -1 non è un residuo quadratico modulo 4. Si potrà allora affermare che l'equazione data non ammette soluzioni.
Fatta questa premessa, concludiamo il capitolo presentando le risoluzioni di alcune equazioni diofantee, a scopo illustrativo e applicativo della teoria finora sviluppata.

Esempio 1.1.1. Dimostrare che l'equazione $x^2 + y^2 = 2015$ non ha soluzioni x, y intere.

Soluzione. Riduciamo l'equazione modulo 4. A destra troviamo 2015 e

$$2015 \equiv 15 \equiv 3 \pmod 4.$$

È possibile che la somma a sinistra sia congrua a 3 modulo 4? Un quadrato è congruo a 0 oppure a 1 modulo 4, quindi $x^2 + y^2$ può essere congruo a 0, a 1 oppure a 2 modulo 4. Ne segue che il primo membro dell'equazione $x^2 + y^2 = 2015$ non può mai essere congruo a 3 modulo 4. Pertanto questa equazione diofantea non ha soluzioni. □

Esempio 1.1.2. Risolvere nei naturali la diofantea $7^x + 1 = 5^y$.

Soluzione. Iniziamo col sostituire alcuni valori a una delle due variabili, per esempio alla y. Se $y = 0$, si ottiene $7^x = 0$ che è impossibile; se $y = 1$, si ottiene

$7^x = 4$ che non ha soluzioni intere; se $y = 2$ si ha $7^x = 24$, ancora priva di soluzioni intere; se $y = 3$ otteniamo $7^x = 124$, impossibile in $\mathbb{N}$. Viene il sospetto che la diofantea non abbia soluzioni. Per dimostrarlo, sfruttiamo il fatto che se un'uguaglianza è vera per gli interi, sarà vera anche la congruenza modulo un intero qualsiasi. In particolare, se $7^x + 1 = 5^y$, allora risulta $7^x + 1 \equiv 5^y \pmod 7$, cioè $1 \equiv 5^y \pmod 7$. Ora, le potenze di 5 modulo 7 sono periodiche di periodo 6, come mostra lo schema sottostante.

k	1	2	3	4	5	6	7	8	9	10	11	12	$\cdots$
$5^k \pmod 7$	5	4	6	2	3	1	5	4	6	2	3	1	$\cdots$

Pertanto, $5^y \equiv 1 \pmod 7$ se e solo se $y = 6h$, $h \in \mathbb{N}$. Sostituendo nell'equazione iniziale si ottiene $7^x + 1 = 5^{6h}$, cioè $7^x = 5^{6h} - 1$, da cui, fattorizzando, si ricava

$$7^x = \left(5^{3h} + 1\right) \cdot \left(5^{3h} - 1\right).$$

Da ciò segue che $h \geq 1$ e che $5^{3h} + 1$ e $5^{3h} - 1$ sono entrambi divisibili per 7 (devono essere due potenze non banali di 7). Di conseguenza è divisibile per 7 anche la loro somma, cioè $2 \cdot 5^{3h}$, e ciò è assurdo. La contraddizione trovata mostra che la diofantea non ha soluzioni. □

Esempio 1.1.3. Risolvere negli interi l'equazione $5x^2 - 3y^2 = 3150$.

Soluzione. Cerchiamo di ricavare informazioni sulla divisibilità delle incognite. Osserviamo, innanzitutto, che il secondo membro è divisibile per 5 e quindi dovrà esserlo anche il primo; di conseguenza y deve essere divisibile per 5, quindi è della forma $y = 5y_1$ per qualche $y_1 \in \mathbb{Z}$. Sostituendo nell'equazione otteniamo

$$5x^2 - 3(5y_1)^2 = 3150$$

da cui, dividendo tutto per 5, si ricava

$$x^2 - 15y_1^2 = 630.$$

Osserviamo ora che 630 è divisibile per 3, quindi anche il primo membro e di conseguenza x dovrà essere divisibile per 3, cioè $x = 3x_1$ per qualche $x_1 \in \mathbb{Z}$. Sostituendo ancora e dividendo ambo i membri per 3 otteniamo

$$3x_1^2 - 5y_1^2 = 210.$$

Ripetendo il ragionamento ricaviamo che $x_1 = 5x_2$, per qualche $x_2 \in \mathbb{Z}$. Sostituendo e semplificando per 5, si ricava

$$15x_2^2 - y_1^2 = 42.$$

Ancora, deve aversi $y_1 = 3y_2$ per qualche $y_2 \in \mathbb{Z}$, che sostituito fornisce la relazione

$$15x_2^2 - 9y_2^2 = 42$$

da cui, semplificando,

$$5x_2^2 - 3y_2^2 = 14.$$

Per ricavare ulteriori informazioni usiamo le congruenze riducendo l'equazione modulo 5, in modo da eliminare un termine. Osservato che $5x_2^2 \equiv 0 \pmod 5$, $-3 \equiv 2 \pmod 5$ e $14 \equiv 4 \pmod 5$, ricaviamo che

$$2y_2^2 \equiv 4 \pmod 5.$$

Di conseguenza, se esiste una soluzione dell'equazione iniziale, essa deve essere tale da verificare, dopo le opportune semplicazioni, la congruenza precedente. Ma osserviamo che, potendo solamente essere $y_2^2 \equiv 0, 1$ oppure 4 modulo 5 risulterà $2y_2^2 \equiv 0, 2$ oppure 3 modulo 5 e quindi non potrà mai verificarsi la relazione $2y_2^2 \equiv 4$ modulo 5. Di conseguenza non esistono soluzioni della diofantea assegnata. □

Esempio 1.1.4. Risolvere negli interi positivi l'equazione

$$\frac{3^m + 3}{2^n + 2^{n-1}} = t.$$

Soluzione. Osserviamo che il problema equivale a determinare tutte le coppie di interi positivi (m, n) tali che $\dfrac{3^m + 3}{2^n + 2^{n-1}}$ sia un intero.
Riscriviamo la frazione $\frac{3^m+3}{2^n+2^{n-1}}$ nel modo seguente.

$$\frac{3^m + 3}{2^n + 2^{n-1}} = \frac{3 \cdot 3^{m-1} + 3}{2^{n-1}(2+1)} = \frac{\cancel{3} \cdot (3^{m-1} + 1)}{\cancel{3} \cdot 2^{n-1}} = \frac{3^{m-1} + 1}{2^{n-1}}.$$

Adesso osserviamo che se $n = 1$ il denominatore della precedente frazione vale 1 e pertanto m può assumere valore qualsiasi. Pertanto una prima classe di soluzioni è data dalle coppie del tipo $(k, 1)$, con $k \geq 1$ intero.
Se $n = 2$, il denominatore della frazione $\frac{3^{m-1}+1}{2^{n-1}}$ vale 2 ed essendo il numeratore $3^{m-1} + 1$ sempre pari qualunque sia $m \geq 1$ intero, ne segue che un'altra classe di soluzioni è data dalle coppie del tipo $(k, 2)$, con $k \geq 1$ intero.
Se $n = 3$, il denominatore della frazione $\frac{3^{m-1}+1}{2^{n-1}}$ vale 4 e quindi, affinchè la stessa frazione sia un intero è necessario e sufficiente che il numeratore sia un multiplo di 4. Pertanto deve aversi $3^{m-1} + 1 \equiv 0 \pmod 4$ ossia $3^{m-1} \equiv 3 \pmod 4$ da cui $3^m \equiv 9 \equiv 1 \pmod 4$.
L'ultima relazione è verificata se e solo se m è pari (se m è dispari si ha $3^m \equiv 3 \pmod 4$) e quindi un'altra classe di soluzioni è data dalle coppie del tipo $(2h, 3)$, con $h \geq 1$ intero.

Se $n = 4$, il denominatore della frazione $\frac{3^{m-1}+1}{2^{n-1}}$ vale 8 e quindi, affinchè la stessa frazione sia un intero è necessario e sufficiente che il numeratore sia un multiplo di 8. Pertanto deve aversi $3^{m-1} + 1 \equiv 0 \pmod 8$ ossia $3^{m-1} \equiv 7 \pmod 4$.
Quest'ultima relazione non è mai verificata in quanto, come facilmente si può dimostrare, 3^k è congruo a 1 oppure a 3 modulo 8. Pertanto il numeratore della frazione data non è mai multiplo di 8 e quindi per $n = 4$ non esistono soluzioni.
Se $n \geq 5$ il problema non ammette soluzioni in quanto il denominatore della frazione $\frac{3^{m-1}+1}{2^{n-1}}$ sarà sempre un multiplo di 8, mentre il numeratore no.
In conclusione le terne di interi positivi (m, n, t) soluzioni dell'equazione assegnata sono tutte le terne del tipo $\left(k, 1, 3^{k-1} + 1\right)$, $\left(k, 2, \frac{3^{k-1}+1}{2}\right)$, $\left(2h, 3, \frac{3^{2h-1}+1}{4}\right)$, con $h, k \geq 1$ interi. □

Problemi proposti

Problema 1.* Risolvere negli interi l'equazione $x^2 - 3y^2 = 17$.

Problema 2.** Risolvere nei naturali l'equazione $x! = 3^y - 1$.

Problema 3.** Risolvere nei naturali l'equazione $3^y - x^2 = 41$.

Problema 4.* Determinare se 7004 può essere scritto come differenza di due cubi perfetti.

Problema 5.** Determinare per quali valori interi di n l'equazione diofantea $n^8 - n^2 = 72m$ è impossibile.

Problema 6.** Trovare tutte le quaterne (x, y, z, a) di interi non negativi tali che $x^2 + y^2 + z^2 = 2^a - 1$.

Problema 7.** Risolvere negli interi l'equazione $x^2 = y^{11} - 3$.

Problema 8.*** Determinare le soluzioni intere dell'equazione

$$19x^3 - 84y^2 = 1984.$$

(MMO, 1984)

Problema 9.*** Trovare tutte le coppie di interi positivi che soddisfano l'equazione $x^2 + 615 = 2^y$ (OliMat, 1995).

Problema 10.*** Trovare tutte le coppie (x, y) di interi non negativi tali che $7^x - 3^y = 4$ (India, 1995).